WEST

End of Result Set

Generate Collection

L3: Entry 1 of 1 File: USPT Jul 2, 1996

US-PAT-NO: 5533123
DOCUMENT-IDENTIFIER: US 5533123 A

TITLE: Programmable distributed personal security

DATE-ISSUED: July 2, 1996

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Force; Gordon	San Jose	CA		
Davis; Timothy D.	Arlington	TX		
Duncan; Richard L.	Bedford	TX		
Norcross; Thomas M.	Arlington	TX		
Shay; Michael J.	Arlington	TX		
Short; Timothy A.	Duncanville	TX		

US-CL-CURRENT: 713/189; 380/2, 380/52, 713/164

CLAIMS:

We claim:
1. A system for processing and storing sensitive information, including messages received and generated by the system and keys used to encrypt and decrypt the messages, and securing the information against potential attacks, the system comprising:
(a) a cryptographic engine for performing cryptographic operations on messages using a first key;
(b) one or more detectors for detecting events characteristic of an attack;
(c) a plurality of potential responses to detected events; and
(d) a programmable filter for correlating detected events with one or more operational factors and for selecting and invoking one or more responses based upon the correlation.
2. A secure cryptographic chip for processing and storing sensitive information, including messages received and generated by the chip and keys used to encrypt and decrypt the messages, and for securing the information against potential attacks, the chip comprising:
(a) a cryptographic engine for performing cryptographic operations on messages using a first key;
(b) one or more detectors for detecting events characteristic of an attack; and
(c) a plurality of potential responses to detected events,
whereby sensitive information is unencrypted only on the chip, where it is secure from attack.
3. The secure cryptographic chip of claim 2, further comprising a key generator for generating a second key used by the cryptographic engine to perform cryptographic operations on the first key.
4. A method for processing and storing sensitive information, including messages and keys used to encrypt and decrypt the messages, and for securing the information against potential attacks, the method comprising the following steps:
(a) performing cryptographic operations on messages using a first key;
(b) detecting one or more events characteristic of an attack; and
(c) responding to the detected events,
whereby sensitive information is unencrypted only on the chip, where it is secure from attack.

5. The method of claim 4, further comprising the steps of:
(a) generating a second key on the chip; and
(b) using the second key to perform cryptographic operations on the first key.
6. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:
(a) an internal system clock for synchronizing functions performed on the chip; and
(b) an external signal synchronizer for synchronizing to the internal system clock all asynchronous external signals received by the chip,
whereby the chip cannot be placed in an unknown state due to the receipt of asynchronous external signals.
7. The secure chip of claim 6 wherein the external signal synchronizer synchronizes asynchronous external signals by accepting and using the signals only at selected times determined by the internal system clock.
8. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:
(a) an internal bus for transferring information among components of the chip;
(b) an input/output port for transferring information between internal components of the chip and external devices; and
(c) a bus monitor for periodically comparing the contents of the input/output port before and after the transfer of information along the internal bus,
whereby the chip can detect unauthorized rerouting, to the input/output port, of sensitive information transferred along the internal bus.
9. The secure chip of claim 8 wherein the bus monitor compares the contents of the input/output port before and after:
(a) a first transfer of less than all of the sensitive information desired to be transferred along the internal bus; and
(b) a second transfer of the remaining sensitive information, if no change in the contents of the input/output port is detected following the first transfer,
whereby the chip can effectively prevent the unauthorized rerouting, to the input/output port, of sensitive information transferred along the internal bus.
10. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:
(a) a real time clock controlled by an external clock crystal having a substantially consistent external clock frequency;
(b) an internal system clock for synchronizing functions performed on the chip, the internal system clock cycle frequency within a predetermined range of accuracy; and
(c) a clock integrity check for
(i) causing the chip to perform a reference operation requiring a predetermined number of internal clock cycles and a predetermined range of expected external clock cycles based upon the range of accuracy of the internal system clock; and
(ii) determining, from the number of internal clock cycles elapsed per actual external clock cycle during the performance of the reference operation, whether the number of elapsed actual external clock cycles lies within the range of expected external clock cycles,
whereby the chip can detect unauthorized tampering with the external clock frequency.
11. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:
(a) a real time clock controlled by an external clock crystal having a substantially consistent external clock frequency, the real time clock having a counter for counting the number of elapsed external clock cycles;
(b) a rollover detector for detecting whether the real time clock counter rolled over; and
(c) a rollover bit, set upon detecting that the real time clock counter rolled over,
whereby, if the rollover bit is set during an operation not expected to require a sufficient number of external clock cycles to cause the counter to roll over, the chip will detect unauthorized tampering with the external clock frequency.
12. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:
(a) a rewritable memory for storing sensitive information;
(b) a power loss detector for detecting that the loss of both system and battery power is imminent; and
(c) a VRT bit for indicating the sufficiency of system and battery power following the loading of sensitive information into the rewritable memory, the VRT bit set upon the loading of the sensitive information into the rewritable memory and reset upon the detection of power loss,

whereby the chip can detect the need to save the sensitive information prior to the actual loss of both system and batter power.

13. The secure chip of claim 12, further comprising a rewritable memory modification detector for detecting modification of the rewritable memory, whereby the chip can detect the need to reload the sensitive information into the rewritable memory.

14. A secure chip for processing sensitive information and securing the information against potential attacks, the chip comprising:

(a) a rewritable memory for storing sensitive information having a substantially constant value;

(b) a memory inverter for periodically inverting the contents of each cell of the rewritable memory; and

(c) a memory state bit for indicating whether the contents of each cell of the rewritable memory are in their actual state, or in the inverted state,

whereby the contents of the rewritable memory contain effectively no residual indication of the constant value of the sensitive information.

WEST

Generate Collection

L5: Entry 2 of 3 File: USPT Sep 28, 1999

US-PAT-NO: 5960082
DOCUMENT-IDENTIFIER: US 5960082 A

TITLE: Post-initialization of chip cards

DATE-ISSUED: September 28, 1999

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Haenel; Walter	Holzgerlingen			DEX

US-CL-CURRENT: 713/172; 235/492, 705/66

CLAIMS:

What is claimed is:
1. Method for post-initializing a chip card, the card having a processor, a non-volatile memory and an operating system with operating commands which are usable in a user operating mode, comprising the acts of:
writing a key for a cryptographic algorithm onto the chip card;
initializing the chip card;
switching over at least once to a post-initialization status from an operating mode,
writing additional data to the chip card in the post-initialization status with the use of the operating commands in conjunction with the key.
2. Method in accordance with claim 1, further comprising:
generating a modified key after operating commands are used in conjunction with the key to write further data onto the chip card after initialization, and
writing additional data onto the chip card with the use of the operating commands in conjunction with the modified key.
3. Method in accordance with claim 2, comprising:
overwriting the key with the modified key.
4. Method in accordance with claim 1, comprising:
writing user-dependent and user-independent data to the chip card in the post-initialization status with the use of the operating commands.
5. Method in accordance with claim 1, comprising:
writing the key during the initialization of the chip card.
6. Method in accordance with claim 1, comprising:
switching the chip card from a personalization mode into the post-initialization status.
7. Method in accordance with claim 1, comprising:
replacing a random number by a fixed numerical value while using the key during the writing of the additional data onto the chip card.
8. Method in accordance with claim 1, comprising:
writing a personalization key onto the chip card during the initialization; and
using the personalization key as the key for the cryptographic algorithm.
9. A chip card having a processor, a non-volatile memory and an operating system with operating commands, and:
upon which data, including user-independent data and applications, is written during initialization of the chip card;
upon which a key for a cryptographic algorithm is written; and
upon which additional data is written after the conclusion of initialization using the operating commands in conjunction with the key.